INFORMATION AND CONTROL 20, 182–187 (1972)

A Class of Low-Rate Nonlinear Binary Codes

A. M. KERDOCK*

Sperry-Rand Corporation, Great Neck, New York

Communicated by E. R. Berlekamp

This paper introduces a new class of nonlinear binary codes. For each $l = 2, 3,...$ we present a code with 2^{4l} codewords of length $N = 4^l$ and distance $d = (4^l - 2^l)/2$. Each code is a supercode of the 1st-order Reed–Muller (RM) code and a subcode of the 2nd-order RM code. These codes are the "duals" of the extended nonlinear Preparata codes in the sense that their weight distributions satisfy the MacWilliams identities.

We assume that the reader is familiar with the Mattson–Solomon polynomials, linearized polynomials, and affine polynomials as discussed in Sections 11.1 and 16.3 of Berlekamp (1968).

We begin with a lemma which often allows us to calculate the weight of a codeword in the 2nd-order RM code from its Mattson–Solomon polynomial.

LEMMA. *Let $f(x)$ be the Mattson–Solomon polynomial of the 2nd-order* RM *codeword $[f(0), f(1), f(\alpha),..., f(\alpha^{2^m-2})]$, where α is a primitive element of $GF(2^m)$ and $f(\xi) \in GF(2)$ for all $\xi \in GF(2^m)$. Then the derivative of $f(x)$ is an affine polynomial of the form*

$$f'(x) = t + L(x),$$

where $t \in GF(2^m)$ and $L(x)$ is a linearized polynomial, and the weight of the codeword with Mattson–Solomon polynomial $f(x)$ is given by

$$|f| = \begin{cases} 2^{m-1} \text{ if } f(\xi) = f(0) + 1 \text{ and } L(\xi) = 0 \text{ for some } \xi \in GF(2^m), \\ 2^{m-1} \pm 2^{m-1-(m-s)/2} \text{ otherwise,} \end{cases}$$

where s is the dimension of the root space of $L(x)$ in $GF(2^m)$.

* This research was partially supported by the Air Force Office of Scientific Research (AFSC) under Contract F44620-71-C-0001. This paper is based upon portions of a dissertation submitted in 1972 to the Faculty of the Polytechnic Institute of Brooklyn, in partial fulfillment of the requirements for the Ph.D. degree in electrical engineering.

Proof. According to Dickson's theorem [cf. Theorem 16.35 of Berlekamp (1968)], every codeword of the 2nd-order RM code has a Mattson–Solomon polynomial of the form

$$f(x) \equiv A + T(ux) + \sum_{i=1}^{h} T(\beta_i x)T(\gamma_i x) \bmod x^{2^m-1} + x, \tag{1}$$

where $A \in GF(2)$, $u \in GF(2^m)$, $T(\xi) = \sum_{i=0}^{m-1} \xi^{2^i}$ and $\beta_1, \gamma_1, \beta_2, \gamma_2, \ldots, \beta_h, \gamma_h$ are certain elements of $GF(2^m)$ which are linearly independent over $GF(2)$. If u is linearly independent of $\beta_1, \gamma_1, \ldots, \beta_h, \gamma_h$, then $|f| = 2^{m-1}$, but if u is a linear combination of $\beta_1, \gamma_1, \ldots, \beta_h, \gamma_h$, then an appropriate affine transformation of the β's and γ's can replace u by 0 and give $|f| = 2^{m-1} \pm 2^{m-1-h}$, where the sign depends on the binary constant A.

Differentiating Eq. (1) gives

$$f'(x) = u + \sum_{i=1}^{h} (\beta_i T(\gamma_i x) + \gamma_i T(\beta_i x)(\beta_i \gamma_i)^{2^{m-1}})$$

$$= u + \sum_{i=1}^{h} (\beta_i \gamma_i^{2^{m-1}} + L(x)),$$

where $L(x)$ is a linearized polynomial.

The equation $L(\xi) = 0$ is equivalent to

$$\sum_{i=1}^{h} (\beta_i T(\gamma_i \xi) + \gamma_i T(\beta_i \xi)) = 0. \tag{2}$$

If $\xi \in GF(2^m)$, then $T(\gamma_i \xi)$ and $T(\beta_i \xi) \in GF(2)$. Since $\beta_1, \gamma_1, \ldots, \beta_h, \gamma_h$ are linearly independent over $GF(2)$, Eq. (2) holds iff

$$T(\gamma_i \xi) = T(\beta_i \xi) = 0 \qquad \text{for} \quad i = 1, 2, \ldots, h. \tag{3}$$

Let $\gamma_1, \beta_1, \ldots, \gamma_h, \beta_h, \delta_1, \delta_2, \ldots, \delta_{m-2h}$ be a basis of $GF(2^m)$ over $GF(2)$. Then ξ is uniquely specified by the m binary values $T(\gamma_i \xi)$, $T(\beta_i \xi)$, $T(\delta_j \xi)$, where $i = 1, 2, \ldots, h$ and $j = 1, 2, \ldots, m - 2h$. Hence there are 2^{m-2h} solutions of Eq. (3), corresponding to the 2^{m-2h} choices of $T(\delta_j \xi)$. Thus $s = m - 2h$ and $h = (m - s)/2$. The proof is completed with the observation that u is linearly independent of γ_i, β_i, $(i = 1, \ldots, h)$ iff there exists a solution of the equations $T(u\xi) = 1$; $T(\gamma_i \xi) = T(\beta_i \xi) = 0$ for $i = 1, \ldots, h$. Q.E.D.

COROLLARY. *If ξ is the "unique" nonzero root of $L(x)$ in $GF(2^m)$, then*

$$|f| = \begin{cases} 2^{m-1} \text{ if } f(\xi) = f(0) + 1, \\ 2^{m-1} \pm 2^{(m-1)/2} \text{ if } f(\xi) = f(0). \end{cases}$$

Code Construction

We now construct our code of length 2^{2l}. Each codeword is defined in terms of two Mattson–Solomon polynomials, one of which specifies the left half of the codeword and the other of which specifies the right half of the codeword. Each half has length 2^m, where $m = 2l - 1$. The left half has Mattson–Solomon polynomial of the form

$$f_l(x) = T(\eta x) + Q(\varphi x) + A$$

and the right half of the same codeword has Mattson–Solomon polynomial of the form

$$f_r(x) = T(\eta x + \varphi x) + Q(\varphi x) + B,$$

where $A, B \in GF(2)$; $\eta, \varphi \in GF(2^m)$ and

$$Q(y) \equiv T(y^3 + y^5 + y^9 + \cdots + y^{1+2^{(m-1)/2}}) \bmod y^{2^m-1} + y$$

We notice in passing that

$$Q'(y) = \sum_{i=1}^{m-1} y^{2^i} = y + T(y) = (T_{m-1}(y))^2,$$

where

$$T_{m-1}(y) = \sum_{i=0}^{m-2} y^{2^i}.$$

Proof that Construction Works

Since there are 2 choices for A, 2 for B, 2^m for η, and 2^m for φ, it is obvious that the construction gives a code with 2^{4l} codewords of length 2^{2l}.

We now show that the difference of any two codewords has weight at least $2^m - 2^{(m-1)/2}$. Let the first codeword have parameters $\eta_1, \varphi_1, A_1, B_1$; the second, $\eta_2, \varphi_2, A_2, B_2$. We define $\varphi_3 = \varphi_1 + \varphi_2$, $\eta_3 = \eta_1 + \eta_2$, $A_3 = A_1 + A_2$, $B_3 = B_1 + B_2$. The left half of the difference then has Mattson–Solomon polynomial

$$\Delta_l(x) = Q(\varphi_1 x) + Q(\varphi_2 x) + T(\eta_3 x) + A_3 \tag{4}$$

and the right half has Mattson–Solomon polynomial

$$\Delta_r(x) = \Delta_l(x) + T(\varphi_3 x) + A_3 + B_3. \tag{5}$$

The case $\varphi_3 = 0$ is trivial, because the difference of the two codewords then has weight 0, 2^m, or 2^{m+1}. (In fact, the difference belongs to the 1st-order RM code of length 2^{m+1} and minimum distance 2^m.) We therefore assume that $\varphi_3 \neq 0$. Since $(\varphi_1 + \varphi_2)/\varphi_3 = 1$ and m is odd, it follows that

$$T(\varphi_1/\varphi_3) + T(\varphi_2/\varphi_3) = T(1) = 1. \tag{6}$$

Furthermore, since

$$(\varphi_1{}^2 + \varphi_1\varphi_2)/\varphi_3{}^2 = \varphi_1/\varphi_3$$

it follows that

$$T(\varphi_1{}^2/\varphi_3{}^2) + T(\varphi_1\varphi_2/\varphi_3{}^2) = T(\varphi_1/\varphi_3),$$

whence

$$T(\varphi_1\varphi_2/\varphi_3{}^2) = 0. \tag{7}$$

From Eqs. (4) and (5) we obtain

$$\Delta_l'(x) = \varphi_1(\varphi_1 x + T(\varphi_1 x)) + \varphi_2(\varphi_2 x + T(\varphi_2 x)) + \eta_3$$

and

$$\Delta_r'(x) = \varphi_1(\varphi_1 x + T(\varphi_1 x)) + \varphi_2(\varphi_2 x + T(\varphi_2 x)) + \eta_3 + \varphi_3 .$$

Both derivatives have linearized part given by

$$L(x) = \varphi_3{}^2 x + \varphi_1 T(\varphi_1 x) + \varphi_2 T(\varphi_2 x).$$

We have $L(\xi) = 0$ iff

$$\xi = [\varphi_1 T(\varphi_1 \xi) + \varphi_2 T(\varphi_2 \xi)]/\varphi_3{}^2.$$

If $\xi \in GF(2^m)$, then $T(\varphi_1\xi)$ and $T(\varphi_2\xi) \in GF(2)$. Hence

$$\xi = \begin{cases} 0 & \text{if } T(\varphi_1\xi) = T(\varphi_2\xi) = 0, \\ \varphi_1/\varphi_3{}^2 & \text{if } T(\varphi_1\xi) = 1 \text{ and } T(\varphi_2\xi) = 0, \\ \varphi_2/\varphi_3{}^2 & \text{if } T(\varphi_1\xi) = 0 \text{ and } T(\varphi_2\xi) = 1, \\ 1/\varphi_3 & \text{if } T(\varphi_1\xi) = 1 \text{ and } T(\varphi_2\xi) = 1. \end{cases} \tag{8}$$

The final possibility, $\xi = 1/\varphi_3$, cannot be realized because it leads to an immediate contradiction of Eq. (6).

If $T(\varphi_1\xi) = 1$, then $\xi = \varphi_1/\varphi_3^2$ and $T(\varphi_2\xi) = 0$ by Eq. (7). Similarly, $T(\varphi_2\xi) = 1$ implies that $T(\varphi_1\xi) = 0$. Hence Eq. (8) may be rewritten as

$$\xi = \begin{cases} 0 \text{ and} \\ \varphi_1/\varphi_3^2 \text{ if } T(\varphi_1/\varphi_3) = 1, \\ \varphi_2/\varphi_3^2 \text{ if } T(\varphi_2/\varphi_3) = 1. \end{cases}$$

From Eq. (6) we deduce that there is always a unique nonzero solution for ξ, which we may write in the form

$$\xi = T(\varphi_1/\varphi_3)(\varphi_1/\varphi_3^2) + T(\varphi_2/\varphi_3)(\varphi_2/\varphi_3^2).$$

According to the Corollary, the weights $|\Delta_l|$ and $|\Delta_r|$ depend on $\Delta_l(\xi)$ and $\Delta_r(\xi)$ which we now compute.

$$\begin{aligned} \Delta_l(\xi) + \Delta_l(0) &= \Delta_r(\xi) + \Delta_r(0) + T(\xi\varphi_3), \\ T(\xi\varphi_3) &= [T(\varphi_1/\varphi_3)]^2 + [T(\varphi_2/\varphi_3)]^2 \\ &= T(\varphi_1/\varphi_3) + T(\varphi_2/\varphi_3) = 1. \end{aligned}$$

It follows that either $|\Delta_l| = 2^{m-1}$ and $|\Delta_r| = 2^{m-1} \pm 2^{(m-1)/2}$ or $|\Delta_l| = 2^{m-1} \pm 2^{(m-1)/2}$ and $|\Delta_r| = 2^{m-1}$. In either case, $|\Delta_l| + |\Delta_r| = 2^m \pm 2^{(m-1)/2}$. Q.E.D.

The preceding proof also shows that all codewords with weight 2^m or 2^{m+1} lie in the 1st-order RM code; all other nonzero codewords have weight $2^m \pm 2^{(m-1)/2}$. Hence, the weight enumerator of our code of length 2^{2l} is given by the polynomial

$$\mathcal{K}(z) = 1 + K_w z^w + (2^{2l+1} - 2)z^{2^{2l-1}} + K_w z^{2^{2l}-w} + z^{2^{2l}},$$

where $w = 2^{2l-1} - 2^{l-1}$ and $K_w = 2^{2l}(2^{2l-1} - 1)$.

Goethals (1971) has observed that the weight distributions of our codes are the "duals" of the weight distributions of the extended Preparata (1968) codes, in the sense that they satisfy the identities of MacWilliams (1963), namely

$$\mathcal{P}(z) = 2^{-4l}(1 + z)^{2^{2l}}\mathcal{K}\left(\frac{1 - z}{1 + z}\right),$$

where $\mathcal{P}(z)$ is the weight enumerator of the extended Preparata code which has 2^{4l} codewords of length 2^{2l} and distance 6. The weight enumerator of the Preparata codes was first given by Semakov and Zinoviev (1969). The sym-

metry groups of our codes are not yet known, except in case $l = 2$, when our construction and Preparata's construction both give the extended Nordstrom–Robinson (1968) code of length 16, whose symmetry group is among those studied by Berlekamp (1971).

Welch (1971) has shown that the linear space spanned by any one of our codes is the full 2nd-order Reed–Muller code of the same length. Mykkeltveit (1972) has demonstrated that the codes are systematic, and that the first $2l$ bits in the right and left halves of the code can be used for the $4l$ information bits.

Acknowledgments

I am indebted to Professor J. K. Wolf for supervising the thesis on which this paper is based and to E. R. Berlekamp for writing this paper.

Revised: September 28, 1971

References

Berlekamp, E. R. (1968), "Algebraic Coding Theory," McGraw-Hill Book Co., New York.

Berlekamp, E. R. (1971), Coding theory and the Mathieu groups, *Information and Control* **18**, 40–64.

Goethals, J. M. (1971), unpublished correspondence.

MacWilliams, F. J. (1963), A theorem of the distribution of weights in a systematic code, *Bell Syst. Tech. J.* **42**, 79–94.

Mykkeltveit, J. (1972), note in JPL Deep Space Net Progress report, unpublished.

Nordstrom, A. W., and Robinson, J. P. (1967), An optimum nonlinear code, *Information and Control* **11**, 613–616.

Preparata, F. P. (1968), A class of optimum nonlinear double-error-correcting codes, *Information and Control* **13**, 378.

Semakov, N. V., and Zinoviev, V. A. (1969), Balanced codes and tactical configurations, *Problemy Peredači Informaci* **5**(3), 28–36 (in Russian).

Welch, L. R. (1971), unpublished correspondence.